

The Geometry of Ideal-specific Elimination-Orders and Improvements to Elimination

Hartwig Bosse

J.W. Goethe Universität, Frankfurt

Christine Gärtner

DFG Research Center MATHEON, Freie Universität Berlin

Abstract

This paper shows that Gröbner walks aiming for the elimination of variables from a polynomial ideal can be terminated much earlier than previously known. To this end we provide an improved stopping criterion for a known Gröbner walk algorithm for the elimination of variables. This results from two new geometric insights on Gröbner fans:

We show that for any given ideal $\mathfrak{J} \subset \mathbb{K}[x_1, \dots, x_n]$ the collection of Gröbner cones corresponding to \mathfrak{J} -specific elimination orders may contain Gröbner cones in the relative interior of the positive orthant. Moreover we prove that the corresponding Gröbner cones form a star-shaped region (the center being the set of all universal elimination vectors) which contrary to first intuition in general is not convex.

Keywords: polynomial ideal, elimination, Groebner basis, Groebner fan, Groebner walk, basis conversion

1. Introduction

Elimination in systems of polynomial equations is a classical topic important in optimization and modeling. Given an ideal \mathfrak{J} of polynomials in $\mathbb{K}[X][U] := \mathbb{K}[x_1, \dots, x_n, u_1, \dots, u_m]$ over some field \mathbb{K} , the task of eliminating the variables u_i can be solved by finding an ideal basis for the the so called *elimination ideal* $\mathfrak{J} \cap \mathbb{K}[X]$, where $\mathbb{K}[X] = \mathbb{K}[x_1, \dots, x_n]$. This can be achieved using resultants (see [11], [9], or [10]), or by calculating a Gröbner basis (GB) for \mathfrak{J} with respect to some special monomial order ([3], [7]), as for example, the pure lexicographic or block term orders. Concerning these approaches, the method using Gröbner-bases has some important advantages, namely, the method is reliable and can algorithmically solve the problem in full generality.

Email addresses: bosse@math.uni-frankfurt.de (Hartwig Bosse),
christine.gaertner@math.fu-berlin.de (Christine Gärtner)

In the Gröbner basis approach one calculates a Gröbner basis $G_{\prec_{\text{elim}}}$ with respect to a suitable monomial order \prec_{elim} , such that those polynomials in $G_{\prec_{\text{elim}}} \cap \mathbb{K}[X]$ form a Gröbner basis for $\mathfrak{I} \cap \mathbb{K}[X]$. Calculating these very specific Gröbner-bases directly, can in practice be rather difficult. Therefore the task of computing such a special GB is usually reduced to performing a Gröbner walk, a method introduced by Collart, Kalkbrener, and Mall in [4].

The actual walk consists of a series of elementary GB-conversions which are easy to compute. Starting with some easily computable GB of \mathcal{I} with respect to some order \prec_{start} , step-by-step, intermediate GBs for orders in between \prec_{start} and \prec_{elim} are calculated. Each basis-conversion from one intermediate GB into the next is (in general) relatively cheap computationwise, keeping the overall amount of necessary calculations relatively low (see [1]).

To handle the intermediate orders in any Gröbner walk algebraically, one represents them by weight-vectors and introduces the concept of a Gröbner fan:

Any proper monomial-order for monomials in $\mathbb{K}[X][U]$ can be represented by some weight-vector in $\omega \in \mathbb{R}_{\geq 0}^{n+m}$. The Gröbner fan, introduced by Mora and Robbiano in [8], is a polyhedral complex, which subdivides the weight vectors in $\mathbb{R}_{\geq 0}^{n+m}$. Each cell of the Gröbner fan is an equivalence class of such weight-vectors:

Two weight-vectors are equivalent, if the monomial order they represent yields the same Gröbner basis for \mathfrak{I} . The closure of such an equivalence class is a *Gröbner cone*, and the overall union of these cones forms the Gröbner fan. Note that Gröbner cones are polyhedral cones (see [8]).

Concerning Gröbner walks used in elimination of variables, Tran proposes in [12] to have the target monomial order \prec_{elim} dependent on \mathfrak{I} , combining the Gröbner walk technique with a sudden-death-algorithm.

So instead of using *the same* elimination term order for *all* ideals, Tran proposes to use *an ideal-specific* monomial order suitable (only) for elimination in the specifically given ideal. He characterizes these ideal-specific orders via the corresponding reduced Gröbner-basis.

In addition to being faster on some examined test bed cases, his approach gets rid of several algebraic technicalities involved in Gröbner walks, such as the necessary perturbation of the weight-vector representing the elimination order:

Gröbner-walk algorithms are particularly fast, if the given path of the walk is *generic*. To achieve this, one has to perturb the target weight vector of the walk in a suitable manner (see e.g. [6]). In [12], Tran observed that using ideal-specific elimination orders, it suffices to end a Gröbner walk in a Gröbner cone adjacent to some *elimination-vector* (see below) which eases the requirements on the necessary perturbations.

We refine Tran's findings by giving a more precise classification of those Gröbner cones, which correspond to ideal-specific elimination orders.

1.1. Main result

The main results of this paper are the following:

For any given ideal $\mathfrak{J} \subseteq \mathbb{K}[x_1, \dots, x_n, u_1, \dots, u_m]$, the union of all Gröbner cones belonging to \mathfrak{J} -specific orders for the elimination of u_1, \dots, u_m from \mathfrak{J} form a star shaped region around the set $\Omega_u = \{\omega \in \mathbb{R}_{\geq 0}^{n+m} : \omega_1 = 0, \dots, \omega_n = 0\}$. This means that if one wishes to eliminate the variables u_i from \mathfrak{J} , i.e., one wants to calculate some Gröbner basis for $\mathfrak{J} \cap \mathbb{K}[X]$, the orders \prec that *do yield* such a Gröbner basis have Gröbner cones, whose union is a star-shaped region around Ω_u .

Moreover we show that some of the Gröbner cones which belong to \mathfrak{J} -specific elimination orders intersect the border of the Gröbner fan in the point zero *only*, meaning that roughly speaking, they are located in the relative interior of the Gröbner fan.

Both results are very useful when trying to eliminate variables using the Gröbner walk-approach: First of all, we can improve the stopping-criterion for such a Gröbner walk relative to the known result of Tran [13]. Moreover, knowing the geometric shape of the target-region can help improve the step-decision process in a Gröbner walk towards an elimination-basis.

Finally, in the general case, just as shown by Tran, using our algorithm, one can get rid of technicalities involved in the implementation of the Gröbner walk such as the perturbation of the target-vector (see [13]).

2. Notation

In the following we introduce some general notation for polynomials and monomial orders. To avoid clashes with our distinct variables x_i and u_j , here we name all variables y_i , assuming $(y_1, \dots, y_{n+m}) = (x_1, \dots, x_n, u_1, \dots, u_m)$. So in the following we consider polynomials $f = \sum_{\alpha} f_{\alpha} y^{\alpha}$ where $y^{\alpha} := \prod_{i=1}^{n+m} y_i^{\alpha_i}$ is a monomial with exponent $\alpha \in \mathbb{N}^{n+m}$ and the coefficients f_{α} are from some field \mathbb{K} .

2.1. Monomial orders and reduced Gröbner-bases

In the following let \prec be some monomial order and $f, g \in \mathbb{K}[Y]$. We denote the *leading term* of f w.r.t. \prec by $\text{lt}_{\prec}(f)$, the *leading monomial* of f is denoted by $\text{lm}_{\prec}(f)$. The set $\text{lt}_{\prec}(G) := \{\text{lt}_{\prec}(g) : g \in G\}$ is called the set of *leading terms* of G .

Let $\mathfrak{J} \subset \mathbb{K}[Y]$ be some polynomial ideal, then the *initial ideal* of \mathfrak{J} w.r.t. \prec is the set $\langle \text{lt}_{\prec}(\mathfrak{J}) \rangle := \langle \{\text{lt}_{\prec}(f) : f \in \mathfrak{J}\} \rangle$.

2.1.1. Reducing polynomials

If $\text{lm}_{\prec}(g) = g_{\alpha} y^{\alpha}$ divides any monomial $f_{\beta} y^{\beta}$ in f , i.e. $\alpha \leq \beta$, then f is reducible by g w.r.t. \prec , the polynomial $f - \frac{f_{\beta} y^{\beta}}{\text{lt}_{\prec}(g)} g$ is called the *reduction* of f by g . In order to make some polynomial f non-reducible by a list of ordered polynomials g_i , one uses the division-algorithm, which repetitively calculates the reduction of f by the g_i .

Definition 2.1. Given an ordered tuple of polynomials $G := (g_1, \dots, g_k)$, using the division algorithm (as in [5], chap. 2, §3) one obtains the remainder $\text{rem}_{\prec}(f, G) \in \mathbb{K}[Y]$ of successive division of f by g_1, \dots, g_k .

The polynomial $\text{rem}_{\prec}(f, G)$ satisfies

$$f = a_1 g_1 + \dots + a_k g_k + \text{rem}_{\prec}(f, G) \quad (1)$$

where $\text{rem}_{\prec}(f, G)$ can *not* be reduced by any of the g_i , i.e., no monomial of $\text{rem}_{\prec}(f, G)$ is divisible by any $\text{lt}_{\prec}(g_i)$ [5]. Moreover, if $f \in \mathfrak{J}$ and $G \subseteq \mathfrak{J}$, then by (1) one finds $\text{rem}_{\prec}(f, G) \in \mathfrak{J}$.

2.1.2. Reduced Gröbner-bases

In this work we consider normed reduced Gröbner-bases: Let $\mathfrak{J} \subseteq \mathbb{K}[Y]$ be some monomial ideal and let \prec be some monomial order. A Gröbner basis G for \mathfrak{J} w.r.t. \prec is called *reduced* if for every pair $g, h \in G$, $g \neq h$ one has that $\text{lm}_{\prec}(g)$ does not divide any monomial of h . Moreover G is called normed if for all $g \in G$ the leading coefficient is 1.

Every ideal $\mathfrak{J} \subseteq \mathbb{K}[Y]$ has a unique finite normed reduced Gröbner basis with respect to \prec (see [5], [2]), which we denote by $\underline{GB}(\mathfrak{J}, \prec)$.

2.2. Weight vectors

To algebraically work with monomial orders, it is helpful to represent them by weight vectors: The set of all *weight vectors* $\Omega := \mathbb{R}_{\geq 0}^{n+m}$ is the non-negative orthant. Let $f \in \mathbb{K}[Y]$ and $\omega \in \Omega$, then $\deg_{\omega}(f) := \max\{\omega^T \alpha : f_{\alpha} \neq 0\}$ is the *degree* of f w.r.t. ω . The *initial form* of f w.r.t. $\omega \in \Omega$ is defined as

$$\text{lt}_{\omega}(f) := \sum_{\alpha \in A} f_{\alpha} y^{\alpha} \quad \text{where} \quad A := \{\alpha \in \mathbb{N}^n : f_{\alpha} \neq 0, \omega^T \alpha = \deg_{\omega}(f)\}.$$

The *initial ideal* of \mathfrak{J} w.r.t. ω is the set $\langle \text{lt}_{\omega}(\mathfrak{J}) \rangle := \langle \{\text{lt}_{\omega}(f) : f \in \mathfrak{J}\} \rangle$.

Definition 2.2. For a fixed ideal $\mathfrak{J} \subseteq \mathbb{K}[Y]$, we say that ω *represents* \prec if $\langle \text{lt}_{\omega}(\mathfrak{J}) \rangle = \langle \text{lt}_{\prec}(\mathfrak{J}) \rangle$ holds.

We say that $\omega \in \Omega$ *refines* a monomial order \prec , if for all pairs of monomials $m_1, m_2 \in [Y]$ one has that $\deg_{\omega}(m_1) < \deg_{\omega}(m_2)$ implies $m_1 \prec m_2$.

Note that any vector ω that *represents* some order \prec is also refined by \prec , the converse does not hold in general [5].

Not all weight vectors ω induce a proper monomial order but using some monomial as an additional tie-breaker does yield an order:

Definition 2.3. Given an ideal $\mathfrak{J} \subseteq \mathbb{K}[Y]$, a monomial order \prec , and some weight-vector ω the monomial order $(\omega | \prec)$ is defined as follows:

Let $\prec' := (\omega | \prec)$, then

$$m_1 \prec' m_2 \quad :\Leftrightarrow \quad \begin{cases} \deg_{\omega}(m_1) < \deg_{\omega}(m_2) \\ \text{or} \quad \deg_{\omega}(m_1) = \deg_{\omega}(m_2) \quad \text{and} \quad m_1 \prec m_2 \end{cases}$$

So $(\omega | \prec)$ corresponds to first (partially) ordering the monomials by \deg_{ω} and using \prec as a tie-breaker.

2.2.1. The Gröbner fan

Definition 2.4. Given an ideal $\mathfrak{J} \subseteq \mathbb{K}[Y]$ and a monomial order \prec , we define the Gröbner cone of \mathfrak{J} w.r.t. by

$$C_{\prec}(\mathfrak{J}) := \text{closure} (\{ \omega \in \Omega : \langle \text{lt}_{\omega}(\mathfrak{J}) \rangle = \langle \text{lt}_{\prec}(\mathfrak{J}) \rangle \})$$

where closure denotes the closure with respect to the standard topology in \mathbb{R}^{n+m} .

For complete information on Gröbner cones, we would like to refer to [8], here we repeat some facts of these cones, relevant to this paper:

Each Gröbner cone of \mathfrak{J} is a convex polyhedral cone with non-empty interior ([8]) and the set of all Gröbner cones forms a polyhedral complex, namely the Gröbner fan $\mathcal{C}(\mathfrak{J}) := \{C_{\prec}(\mathfrak{J}) : \prec \text{ is some monomial order}\}$.

Moreover, each Gröbner cone corresponds to some reduced Gröbner-basis, i.e., all monomial orders, which are represented by the weight vectors within the same Gröbner cone, will have the same reduced Gröbner-basis. This implies that \mathfrak{J} has only finitely many different Gröbner cones. Moreover we obtain we obtain the following relations between the Gröbner cone of some monomial order \prec and the vectors contained in this cell:

Corollary 2.5. *For a weight vector $\omega \in \Omega$ and some order \prec one has the following:*

$$\prec \text{ refines } \omega \Leftrightarrow \omega \in C_{\prec}(\mathfrak{J}) \quad (2)$$

$$\omega \text{ represents } \prec \Leftrightarrow \omega \in \text{int}(C_{\prec}(\mathfrak{J})) \quad (3)$$

Moreover, if $(\omega | \prec) = \prec$ holds, then one has $\omega \in C_{\prec}(\mathfrak{J})$.

Here $\text{int}(C)$ denotes the interior of C with respect to the standard topology. The implications in Corollary 2.5 follow directly from the definitions of the Gröbner cone, for a proof see [4].

2.3. Geometry

In the following we prove that some special set of weight-vectors is star-shaped, to this end we recall the following:

Definition 2.6. A set $S \subseteq \mathbb{R}^{n+m}$ is called *star-shaped* with center $C \subseteq S$, if for any two points $s \in S$ and $c \in C$ the section \overline{ms} is contained in S .

2.4. Universal elimination orders

In the following we assume \mathfrak{J} to be some ideal in $\mathbb{K}[X][U]$. A class of monomial orders, which provides a reduced Gröbner basis for the elimination ideal is the set of elimination orders; these orders are traditionally used to calculate the elimination Ideal via Gröbner-bases.

Definition 2.7. A monomial order \prec on $\mathbb{K}[X][U]$ is called *universal elimination order* for U , if

$$\text{lt}_{\prec}(f) \in \mathbb{K}[X] \quad \Rightarrow \quad f \in \mathbb{K}[X] \quad \forall f \in \mathbb{K}[X][U].$$

For example, the lexicographic order is a universal elimination order. Note that a universal elimination order can be used to calculate the GB of the elimination ideal for *any* given ideal:

Lemma 2.8. *If \prec is a universal elimination order, then for every ideal \mathfrak{J} , the set $\underline{GB}(\mathfrak{J}, \prec) \cap \mathbb{K}[X]$ is the reduced Gröbner basis of the elimination ideal $\mathfrak{J} \cap \mathbb{K}[X]$.*

For a proof see [12].

2.5. Ideal-specific elimination orders

In contrast to universal elimination orders, in this paper we examine ideal-specific elimination orders, which serve to eliminate variables only for the specifically given ideal:

Definition 2.9. (Ideal-specific elimination orders and vectors)
Let $\mathfrak{J} \subseteq \mathbb{K}[X][U]$ be an ideal and \prec a monomial order with

$$\text{lt}_{\prec}(g) \in \mathbb{K}[X] \quad \Rightarrow \quad g \in \mathbb{K}[X] \quad \forall g \in \underline{GB}(\mathfrak{J}, \prec).$$

1. Then \prec is called *\mathfrak{J} -specific elimination order for the elimination of U* .
When clear which variables are to eliminate we abbreviate this to *\mathfrak{J} -specific elimination order*, or just *\mathfrak{J} -EO*.
2. Any $\omega \in C_{\prec}(\mathfrak{J})$ is called *\mathfrak{J} -specific for the elimination of U (\mathfrak{J} -EV)*.

Lemma 2.10. *Let $\mathfrak{J} \subseteq \mathbb{K}[X][U]$ be some fixed ideal. If \prec is an \mathfrak{J} -specific elimination order for the elimination of U , then the set $\underline{GB}(\mathfrak{J}, \prec) \cap \mathbb{K}[X]$ is the reduced Gröbner basis of the elimination ideal $\mathfrak{J} \cap \mathbb{K}[X]$.*

For a proof see [13].

So any \mathfrak{J} -EO will yield a Gröbner basis suitable for the elimination of the variables u_i from \mathfrak{J} . But in contrast to *universal* elimination orders, an \mathfrak{J} -EO will in general not work for other polynomial ideals. However, any *universal* elimination order is -by definition- also an \mathfrak{J} -EO for any ideal \mathfrak{J} .

By Definition 2.9, if \prec is an \mathfrak{J} -EO, then any weight-vector in the Gröbner cone $C_{\prec}(\mathfrak{J})$ is \mathfrak{J} -EV. The reverse statement holds for weight-vectors in the interior of a Gröbner cone and for some weight-vectors $\omega \neq 0$ on the boundary of Ω as Lemmas 2.11 and 2.12 show:

Lemma 2.11. *Let $\mathfrak{J} \subseteq \mathbb{K}[X][U]$ be an ideal, \prec some monomial order and let ω be some weight-vector representing \prec , i.e., $\omega \in \text{int}(C_{\prec}(\mathfrak{J}))$. Then \prec is \mathfrak{J} -EO if and only if ω is an \mathfrak{J} -EV.*

This lemma follows directly from the definition of ω representing \prec . For a complete proof we refer to [13].

The following lemma found in [12] is used to obtain the main result in [13], it shows that for any ideal \mathfrak{J} all *universal* EVs are \mathfrak{J} -EVs, too. Geometrically, Lemma 2.12 proves that \prec is \mathfrak{J} -EO if its Gröbner fan contains points on the boundary of Ω (the non-negative orthant) with positive values.

Lemma 2.12. *Let $\mathfrak{J} \subseteq \mathbb{K}[X][U]$ be some ideal and \prec some monomial order. If $(0, \tilde{\omega}) \in C_{\prec}(\mathfrak{J})$ holds for $\tilde{\omega} \in \mathbb{R}_{>0}^m$, then \prec is an \mathfrak{J} -EO.*

Proof: See [12].

Since each $C_{\prec}(\mathfrak{J})$ containing some vector $(0, \tilde{\omega})$ with $\tilde{\omega} > 0$ comes from some \mathfrak{J} -EO \prec , and since these Gröbner cones are closed, one concludes from Lemma 2.12 that all vectors of the form $(0, \bar{\omega})$, $\bar{\omega} \in \mathbb{R}_{\geq 0}^m$ are in fact \mathfrak{J} -EVs.

3. Main result

Our main result is the following:

Theorem 1. *Let \mathfrak{J} be a polynomial ideal in $\mathbb{K}[x_1, \dots, x_n, u_1, \dots, u_m]$. The Gröbner cones of all \mathfrak{J} -specific elimination orders for the elimination of u_1, \dots, u_m from \mathfrak{J} form a star-shaped region around the following face of $\mathbb{R}_{\geq 0}^{n+m}$:*

$$\Omega_u := \{\omega \in \mathbb{R}_{\geq 0}^{n+m} : \omega_1 = 0, \dots, \omega_n = 0\}$$

In order to prove this result (see page 16) we start with some \mathfrak{J} -EV σ and some point $\tau \in \Omega_u$. We then examine each intermediate (reduced) Gröbner basis G arising in a Gröbner walk from σ to τ . We need to prove that each of these fulfills the prerequisites of Definition 2.9, which in turn implies that $G \cap \mathbb{K}[X]$ is a Gröbner basis for $\mathfrak{J} \cap \mathbb{K}[X]$. To achieve all this, we will examine how Buchberger's algorithm calculates the intermediate Gröbner-bases from a reduced Gröbner basis with respect to the order \prec_{σ} (see Lemmas 4.8 and 4.9). Before we do so, we present a brief consequence of Theorem 1.

3.1. The elimination algorithm by Tran

The algorithm of Tran (Algorithm 1 in [13]) which calculates a Gröbner basis for the elimination ideal by means of a Gröbner walk can be significantly improved, by changing the termination criterion:

Tran proves that monomial orders whose Gröbner cones are on the boundary of the Gröbner fan are ideal-specific elimination-orders. He then sets his algorithm to terminate when reaching such a cell. In Lemma 4.1 we prove that there are ideals \mathfrak{J} , for which there are \mathfrak{J} -specific elimination orders, whose Gröbner cones lie in the relative interior of the Gröbner fan. In this regard, our Algorithm 1 is an improvement of Tran's version.

Algorithm 1. (Improved elimination algorithm)

Input $F = \{f_1, \dots, f_m\} \subseteq \mathbb{K}[X][U]$
 $\tau \in \Omega$, where $\tau^T = (0^T, \gamma^T)$ with $\gamma \in \mathbb{R}_{>0}^m$,
 $\sigma \in \Omega$, such that $\overline{\sigma\tau}$ is generic,
 \prec_σ, \prec_τ refining σ resp. τ .

Output $G \subseteq \mathbb{K}[X]$, reduced Gröbner basis of $\langle F \rangle \cap \mathbb{K}[X]$
w.r.t. some $\langle F \rangle$ -specific. EO for U .

Init Calculate reduced start GB $G_0 := \underline{GB}(\langle F \rangle, \prec_\sigma)$
 $k := 0$, $\mathcal{J} := \langle F \rangle$, $\omega_0 := \sigma$, $\prec_0 := \prec_\sigma$

Step 1 IF \prec_k is \mathcal{J} -EO RETURN $G := G_k \cap \mathbb{K}[X]$

Step 2 $\left\{ \begin{array}{l} \text{GB-walk: change cell} \\ (2.1) \quad k := k + 1 \\ (2.2) \quad \text{Find next weight vector } \omega_k \in \overline{\sigma\tau}, \\ \quad \text{s.t. } \overline{\omega_{k-1}\omega_k} = \overline{\omega_{k-1}\tau} \cap C_{\prec_{k-1}}(\mathcal{J}). \\ (2.3) \quad \text{Set } \prec_k := (\omega_k | \prec_\tau). \\ (2.3) \quad \text{Convert } G_{k-1} \text{ into Gröbner basis } G_k \text{ w.r.t. } \prec_k. \\ (2.4) \quad \text{Interreduce } G_k. \end{array} \right.$

Step 3 GOTO Step 1

Algorithm 1 as stated above, is in fact Tran's Algorithm in [13] with a refined stopping-criterion.

Theorem 2. *Algorithm 1 terminates and is correct.*

Proof. In each ω_k the section $\overline{\sigma\tau}$ crosses from some Gröbner cone into another. Since there are only finitely many such transition-points ω_k , the algorithm must terminate after a finite amount of steps. In case the algorithm stops before it reaches τ , it terminates after calculating the reduced GB G_k for some $\langle F \rangle$ -specific elimination order, so $G_k \cap \mathbb{K}[X]$ is a Gröbner basis for $\langle F \rangle \cap \mathbb{K}[X]$ (see Lemma 2.10).

Note that τ is on the border of the Gröbner fan Ω and thus τ is a valid choice as one of the ω_k . If the algorithm does not terminate before it reaches the end of $\overline{\sigma\tau}$, then in the final ℓ -th step, it assigns $\omega_\ell := \tau$. Subsequently \prec_ℓ is \mathcal{J} -EO: Since \prec_τ refines τ , one has $\prec_\ell := (\tau | \prec_\tau) = \prec_\tau$ and $\tau \in C_{\prec_\tau}(\mathcal{J})$ by Corollary 2.5. By $\tau \in \Omega_u$, Lemma 2.11 implies that \prec_ℓ is \mathcal{J} -EO, meaning that $\underline{GB}(\langle F \rangle, \prec_n) \cap \mathbb{K}[X]$ is a Gröbner basis for $\langle F \rangle \cap \mathbb{K}[X]$. \square

4. The geometry of ideal-specific elimination vectors

In this section we prove three geometrical properties of the set of all elimination vectors for a given ideal.

We prove that for a given ideal \mathfrak{J} , the \mathfrak{J} -specific elimination vectors form a set that is star-shaped. Moreover, we prove that this set in general is non-convex. Finally, we prove by example that an ideal \mathfrak{J} can have an \mathfrak{J} -specific elimination order \prec , whose Gröbner cone $C_{\prec}(\mathfrak{J})$ is -roughly speaking- in the interior of the Gröbner fan of \mathfrak{J} . By the latter we mean that $C_{\prec}(\mathfrak{J})$ intersects the exterior of Gröbner fan of \mathfrak{J} in the origin only.

4.1. Cones in the interior

Lemma 4.1. *There are ideals $\mathfrak{J} \subset \mathbb{K}[X][U]$ which have an \mathfrak{J} -EO \prec whose Gröbner cone $C_{\prec}(\mathfrak{J})$ intersects the boundary of the Gröbner fan in the origin 0 only.*

Proof. Consider the following ideal $\mathfrak{J} = \langle x^2 - 1, xu^2 - x - u \rangle \subseteq \mathbb{K}[x][u]$. There are exactly three different reduced Gröbner-bases of \mathfrak{J} , which correspond to the three Gröbner cones of the Gröbner fan:

$$\begin{aligned} G_1 &= \{\mathbf{x}^2 - 1, \mathbf{u}^2 - xu - 1\} \\ G_2 &= \{\mathbf{x}^2 - 1, \mathbf{xu} - u^2 + 1, \mathbf{u}^3 - 2u - x\} \\ G_3 &= \{\mathbf{x} + 2u - u^3, \mathbf{u}^4 - 3u^2 + 1\} \end{aligned}$$

Here the leading terms are given in bold letters.

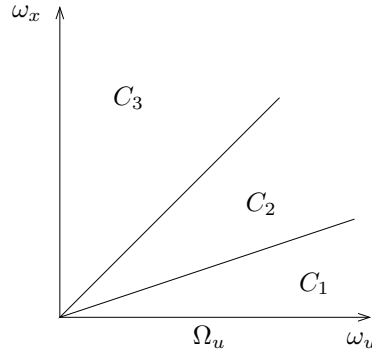


Figure 1: Gröbner fan of $\mathfrak{J} = \langle x^2 - 1, xu^2 - x - u \rangle$

For $i = 1, 2, 3$ let C_i be the Gröbner cones corresponding to the Gröbner base G_i and let \prec_i be some corresponding monomial order.

Examining the polynomials in G_1 and G_2 in respect to Definition 2.9, one observes that \prec_1 and \prec_2 are \mathfrak{J} -specific EOs for the elimination of u . We now check that the cone C_2 must be in between the cones C_1 and C_3 (see Figure 1):

It is easy to check that for $\bar{\omega} := (1, 0)^T$ one has $\text{lt}_{\bar{\omega}}(G_3) = \text{lt}_{\prec_3}(G_3)$ and $\text{lt}_{\bar{\omega}}(G_i) \neq \text{lt}_{\prec_i}(G_i)$ for $i = 1, 2$. This implies that $\bar{\omega} \in C_3$ holds. In the same way one proves $(0, 1)^T \in C_1$.

Since the Gröbner fan considered here is two-dimensional, C_2 must thus be in between C_1 and C_3 . This proves that for \mathfrak{J} , there is indeed an \mathfrak{J} -EO (\prec_2) whose

Gröbner cone (C_2) is in the interior of the Gröbner fan, i.e., C_2 intersects the boundary of the Gröbner fan in $(0, 0)^T$ only. \square

4.2. Non-convexity

It seems intuitive at first sight that the set of all \mathfrak{J} -EVs should be convex, but this is in general not true.

Example 4.2. Let $\mathfrak{J} := \langle x + u + v, x^2 - 1 \rangle \subseteq \mathbb{K}[x][u, v]$ and set $\sigma := (9, 12, 0)^T$, $\tau := (9, 0, 10)^T \in \Omega$, and $\omega := \frac{1}{2}\sigma + \frac{1}{2}\tau = (9, 6, 5)^T \in \overline{\sigma\tau}$. Let \prec_σ, \prec_τ and \prec_ω be monomial orders represented by σ, τ , and ω respectively.

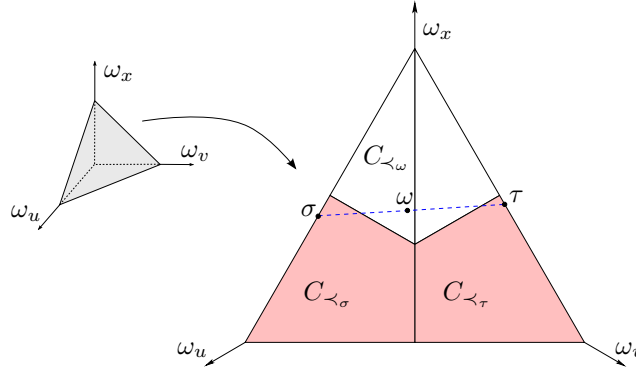


Figure 2: Gröbner fan for $\mathfrak{J} = \langle x + u + v, x^2 - 1 \rangle$

Quick calculation shows that the reduced Gröbner-bases w.r.t. \prec_σ and \prec_τ are the following

$$\begin{aligned} \underline{GB}(\mathfrak{J}, \prec_\sigma) &= \{\mathbf{u} + x + v, \mathbf{x}^2 - 1\}, \\ \underline{GB}(\mathfrak{J}, \prec_\tau) &= \{\mathbf{v} + x + u, \mathbf{x}^2 - 1\}. \end{aligned}$$

So by Definition 2.9, both σ and τ are \mathfrak{J} -specific elimination vectors for elimination of the variables $\{u, v\}$. The reduced Gröbner basis w.r.t \prec_ω is

$$\underline{GB}(\mathfrak{J}, \prec_\omega) = \{\mathbf{x} + u + v, \mathbf{u}^2 + 2uv + v^2 - 1\}.$$

Since one has $\text{lt}_{\prec_\omega}(x + u + v) = x \in \mathbb{R}[x]$ but $x + u + v \notin \mathbb{R}[x]$, by Definition 2.9, \prec_ω can not be \mathfrak{J} -specific for the elimination of u and v .

Figure 2 depicts the Gröbner fan of \mathfrak{J} (intersected with some appropriate hyperplane) together with σ, ω and τ . The highlighted Gröbner cones $C_{\prec_\sigma}, C_{\prec_\tau}$ correspond to the \mathfrak{J} -EOs \prec_σ and \prec_τ .

4.3. Ideal-specific elimination vectors form a star shaped region

Theorem 1, the main result of this work, states that for every polynomial ideal $\mathfrak{J} \subseteq \mathbb{K}[X][U]$ the set of all \mathfrak{J} -EVs which eliminate U from \mathfrak{J} is star-shaped with center $\Omega_u := \{\omega \in \Omega \mid \omega_1, \dots, \omega_n = 0\}$. Note that the corresponding center Ω_u is the set of all *universal elimination* vectors, for a definition see [13].

4.3.1. A generic walk from an \mathfrak{I} -EV to Ω_u

In order to prove Theorem 1 (see page 16), we examine what happens during a Gröbner walk from some \mathfrak{I} -EV σ to some $\tau \in \Omega_u$. We first examine *generic* walks $\overline{\sigma\tau}$ in the Gröbner fan. In this setting, we analyse what happens during a single basis-conversion step during the walk. To do so, we choose an intermediate point $\omega \in \overline{\sigma\tau}$ which represents some intermediate monomial order. Algebraically this translates to the following:

General Assumptions 4.3. In Section 4.3 we use the following general assumptions: Let \prec_σ be some \mathfrak{I} -EO and let $\tau \in \Omega_u$. Moreover let $\sigma \in \text{int}(C_{\prec_\sigma}(\mathfrak{I}))$ be such, that $\overline{\sigma\tau}$ is a generic Gröbner walk.

Let $\omega \in \overline{\sigma\tau}$ be such that ω represents some order \prec_ω , i.e., $\omega \in \text{int}(C_{\prec_\omega}(\mathfrak{I}))$.

To classify the intermediate points $\omega \in \overline{\sigma\tau}$, we calculate the reduced Gröbner base w.r.t. \prec_ω using Bucherberger's algorithm (see [2]) followed by a subsequent interreducing algorithm. When examining the new reduced Gröbner-basis, we look at those polynomials of the Gröbner basis $\mathcal{G} = \underline{GB}(\mathfrak{I}, \prec_\sigma)$ whose monomials reshuffle when ordered according to the new intermediate order (see Corollary 4.5). Combining this analysis with knowledge on the polynomials of \mathcal{G} , one can prove that \prec_ω is an \mathfrak{I} -specific elimination order - which implies that ω (and thus each weight-vectors on the Gröbner walk) is an \mathfrak{I} -specific elimination weight-vector.

The following lemma demonstrates, how monomials behave when sorted according to σ resp. ω :

Lemma 4.4. *Let $\sigma \in \Omega$ be some \mathfrak{I} -EV and $\tau \in \Omega_u$. Then for $\omega \in \overline{\sigma\tau} \setminus \{\tau\}$ and exponents $\alpha, \gamma \in \mathbb{N}_{\geq 0}^n$ and $\beta \in \mathbb{N}_{\geq 0}^m$ one finds*

$$\begin{aligned} \deg_\sigma(x^\alpha u^\beta) &> \deg_\sigma(x^\gamma) \\ \Rightarrow \deg_\omega(x^\alpha u^\beta) &> \deg_\omega(x^\gamma). \end{aligned}$$

Proof. Let $\sigma = (\sigma_x, \sigma_u)$ and $\tau = (0, \tau_u)$ with $\sigma_x \in \mathbb{R}_{\geq 0}^n$ and $\sigma_u, \tau_u \in \mathbb{R}_{\geq 0}^m$. Let moreover $\omega = t \cdot \sigma + (1-t) \cdot \tau$ where $t \in (0, 1]$.

$$\begin{aligned} &\deg_\sigma(x^\alpha u^\beta) > \deg_\sigma(x^\gamma) \\ \Leftrightarrow &\sigma_x^T \alpha + \sigma_u^T \beta > \sigma_x^T \gamma \\ \Rightarrow &t \sigma_x^T \alpha + t \sigma_u^T \beta + (1-t) \tau_u^T \beta > t \sigma_x^T \gamma \quad (\text{since } \tau_u \geq 0 \text{ and } \beta \geq 0) \\ \Leftrightarrow &\deg_\omega(x^\alpha u^\beta) > \deg_\omega(x^\gamma) \end{aligned}$$

Note that for $\beta = 0$ the reverse implication is true, i.e., for $\beta = 0$ one finds

$$\deg_\sigma(x^\alpha) \geq \deg_\sigma(x^\gamma) \Leftrightarrow \deg_\omega(x^\alpha) \geq \deg_\omega(x^\gamma).$$

□

Lemma 4.4 implies the following; Let $p \in \mathbb{K}[X][U]$ be some polynomial. If p contains some monomial $p_\alpha x^\alpha \in \mathbb{K}[X]$ which is *not* in the initial form of p w.r.t. σ , then $p_\alpha x^\alpha$ is also *not* in the initial form of p w.r.t. $\omega \in \overline{\sigma\tau}$. Conversely this means the following:

Corollary 4.5. *Let σ, τ and ω be as in the general Assumptions 4.3. Then for any $p \in \mathbb{K}[X][U]$ one finds*

$$lt_{\omega}(p) \in \mathbb{K}[X] \quad \Rightarrow \quad lt_{\sigma}(p) = lt_{\omega}(p) \in \mathbb{K}[X]$$

Proof. The statement in Corollary 4.5 is a direct consequence of Lemma 4.4. Assume $lt_{\omega}(p) = x^\alpha \in \mathbb{K}[X]$ for some $p \in \mathbb{K}[X][U]$, then by Lemma 4.4, one can not have $lt_{\sigma}(p) = x^\beta u^\gamma$ unless $\beta = \alpha$ and $\gamma = 0$, since otherwise by $\deg_\sigma(x^\beta u^\gamma) > \deg_\sigma(x^\alpha)$ one had $\deg_\omega(x^\beta u^\gamma) > \deg_\omega(x^\alpha)$ in contradiction to $lt_{\omega}(p) = x^\alpha$. \square

After clarifying which monomials of some polynomial might change place, when being resorted by σ as opposed to being ordered by ω , we now deduce what this implies for the polynomials calculated in some basis-conversion along a Gröbner walk. More precisely, during such conversions we trace those polynomials with a leading-term in $\mathbb{K}[X]$:

Definition 4.6. For any set $G \subseteq \mathbb{K}[X][U]$ and for some monomial order \prec we set

$$L_\prec^{[X]}(G) := \{p \in G : lt_\prec(p) \in \mathbb{K}[X]\}.$$

Remark. Definition 4.6 implies: A monomial order \prec is an \mathfrak{J} -EO, if and only if $L_\prec^{[X]}(\underline{GB}(\mathfrak{J}, \prec)) \subseteq \mathbb{K}[X]$ holds (see Definition 2.9).

4.3.2. Basis conversions via Buchberger's algorithm

In the following we examine the reduced GB obtained in a single basis-conversion during a Gröbner walk. To keep things tractable, we calculate the new reduced GB via Buchberger's algorithm and a subsequent reduction, which are both easy to analyse. In a real-world application, one would clearly do a computationally much cheaper basis-conversion, which nevertheless results in the same unique, reduced GB.

Since our analysis specifically examines various steps of both the Buchberger and the interreduce-algorithm, we restate both algorithms in short form. Note that the interreduce step is crucial to the analysis, since using Definition 2.9 one can only tell from a reduced GB whether the corresponding monomial order is an \mathfrak{J} -EO.

Algorithm 2. Buchberger-Algorithm

Input $\{f_1, \dots, f_r\} \subseteq \mathbb{K}[X][U]$, some monomial order \prec

Output Gröbner basis G of $\mathfrak{J} = \langle G_0 \rangle$ w.r.t. \prec

Step 1 $k := 0, G_0 = \{f_1, \dots, f_r\}$

Step 2 REPEAT

- (2.1) $k := k + 1, H := G_{k-1}$
- (2.2) For every pair $(p, q) \in G_{k-1}, p \neq q$
 - (2.2.1) calculate $s := \text{rem}_{\prec}(S_{\prec}(p, q), G_{k-1})$.
 - (2.2.2) if $s \neq 0$ then $H := H \cup \{s\}$
- (2.3) $G_k := H$

UNTIL $G_k = G_{k-1}$

Step 3 RETURN G

The S -Polynomial in Step (2.2.1) of the algorithm is defined as usual by

$$S_{\prec}(p, q) := \frac{x^{\gamma}}{\text{lt}_{\prec}(p)}p - \frac{x^{\gamma}}{\text{lt}_{\prec}(q)}q \quad \text{where } x^{\gamma} := \text{lcm}(\text{lm}_{\prec}(p), \text{lm}_{\prec}(q)),$$

i.e., x^{γ} is the least common multiple of the monomials $\text{lm}_{\prec}(p)$ and $\text{lm}_{\prec}(q)$.

Lemma 4.7. *In addition to the general Assumptions 4.3 let $\mathcal{G} = \underline{GB}(\mathfrak{J}, \prec_{\sigma})$ be the reduced Gröbner basis of \mathfrak{J} w.r.t. \prec_{σ} . Then one has*

$$\begin{aligned} \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}) &= \mathbb{L}_{\prec_{\omega}}^{[X]}(\mathcal{G}) \quad \text{and} \\ \text{lt}_{\prec_{\sigma}}(g) &= \text{lt}_{\prec_{\omega}}(g) \quad \forall g \in \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}). \end{aligned}$$

Proof. Since \prec_{σ} is an \mathfrak{J} -EO, one has $\mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}) \subseteq \mathbb{K}[X]$ and thus for all $p \in \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$ one must find $\text{lt}_{\prec_{\omega}}(p) \in \mathbb{K}[X]$. This implies

$$\mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}) \subseteq \mathbb{L}_{\prec_{\omega}}^{[X]}(\mathcal{G}).$$

By Corollary 4.5, for every $g \in \mathcal{G}$ one has

$$\text{lt}_{\prec_{\sigma}}(g) \in \mathbb{K}[X][U] \setminus \mathbb{K}[X] \quad \Rightarrow \quad \text{lt}_{\prec_{\omega}}(g) \in \mathbb{K}[X][U] \setminus \mathbb{K}[X]$$

This implies

$$\mathbb{L}_{\prec_{\omega}}^{[X]}(\mathcal{G}) \subseteq \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}),$$

proving $\mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}) = \mathbb{L}_{\prec_{\omega}}^{[X]}(\mathcal{G})$.

Now let $g \in \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$, then since \prec_{σ} is an \mathfrak{J} -EO, one has $g \in \mathbb{K}[X]$. By Corollary 4.5 one concludes that the monomials within g obtain the same order when sorted w.r.t. \prec_{σ} as when sorted w.r.t. \prec_{ω} . This implies

$$\text{lt}_{\prec_{\sigma}}(g) = \text{lt}_{\prec_{\omega}}(g) \quad \forall g \in \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}).$$

□

Lemma 4.8. *In addition to the general Assumptions 4.3, let $\mathcal{G} = \underline{GB}(\mathfrak{J}, \prec_\sigma)$. In Algorithm 2 with inputs \mathcal{G} and \prec_ω , let G_k be the sets of polynomials calculated in step (2.3). Then one finds*

$$\begin{aligned} \mathbb{L}_{\prec_\omega}^{[X]}(G_k) &= \mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G}) & \forall k \geq 0 & \quad \text{and} \\ \text{lt}_{\prec_\omega}(g) &= \text{lt}_{\prec_\sigma}(g) & \forall g \in \mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G}). \end{aligned}$$

Proof. The the second claim of Lemma 4.8 is a consequence of Corollary 4.5 and the properties of \mathcal{G} . Namely, since \prec_σ is \mathfrak{J} -EO, one finds that for $g \in \mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G})$ one has $g \in \mathbb{K}[X]$ and thus $\text{lt}_{\prec_\omega}(g) \in \mathbb{K}[X]$. The latter together with Corollary 4.5 proves $\text{lt}_{\prec_\omega}(g) = \text{lt}_{\prec_\sigma}(g)$.

Note that Algorithm 2 only adds polynomials to the basis, none are ever removed. This implies $\mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G}) \subseteq \mathcal{G} \subseteq G_k$ for all k . Moreover, by Assumptions 4.3, \prec_σ is \mathfrak{J} -EO which by definition implies $\mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G}) \subseteq \mathbb{K}[X]$ and thus $\mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G}) \subseteq \mathbb{L}_{\prec_\omega}^{[X]}(G_k)$ for all k .

To show the reverse inclusion, fix some G_k arising in Algorithm 2, with $k > 0$. In regard of step (2.2.1), we need to show that for all $p, q \in G_{k-1}$ with $p \neq q$ the (reduced) s-polynomial $s = \text{rem}_{\prec_\omega}(S_{\prec_\omega}(p, q), G_{k-1})$ fulfills *either* $s = 0$ *or* $\text{lt}_{\prec_\omega}(s) \in \mathbb{K}[X][U] \setminus \mathbb{K}[X]$.

Assume that $\text{lt}_{\prec_\omega}(s) = x^\alpha$ holds. We show the following contradiction: there is $h \in \mathbb{L}_{\prec_\omega}^{[X]}(G_{k-1})$ that reduces s .

By Corollary 4.5 one concludes $\text{lt}_{\prec_\sigma}(s) = \text{lt}_{\prec_\omega}(s) = x^\alpha$. Note that $s \in \mathfrak{J}$, so since \mathcal{G} is a GB for \mathfrak{J} w.r.t. \prec_σ , there is some polynomial $h \in \mathcal{G} \subseteq G_{k-1}$ such that $\text{lt}_{\prec_\sigma}(h)$ divides $\text{lt}_{\prec_\sigma}(s)$. This implies $\text{lt}_{\prec_\sigma}(h) \in \mathbb{K}[X]$ and thus $h \in \mathbb{K}[X]$ since \prec_σ is \mathfrak{J} -EO. This in turn means that $\text{lt}_{\prec_\omega}(h) \in \mathbb{K}[X]$ holds which by Corollary 4.5 implies $\text{lt}_{\prec_\omega}(h) = \text{lt}_{\prec_\sigma}(h)$.

Therefore s can be reduced by $h \in G_{k-1}$ w.r.t. \prec_ω . This conflicts with the assumption $s = \text{rem}_{\prec_\omega}(S_{\prec_\omega}(p, q), G_{k-1})$, since such an s can not be reduced by any polynomial in G_{k-1} w.r.t. \prec_ω . This implies

$$\mathbb{L}_{\prec_\omega}^{[X]}(G_k) = \mathbb{L}_{\prec_\sigma}^{[X]}(\mathcal{G}).$$

□

Algorithm 3. Interreduce-Algorithm

Input A Gröbner basis $\mathcal{H} \subset \mathbb{K}[X][U]$ for some ideal \mathfrak{I} w.r.t. some monomial order \prec

Output $\underline{GB}(\mathfrak{I}, \prec)$, the reduced Gröbner basis of \mathfrak{I} w.r.t. \prec

Step 1 $H := \mathcal{H}$

Step 2 REPEAT

(2.1) $\overline{H} := H$

(2.1) For each $p \in \overline{H}$

(2.2.1) calculate $p' := \text{rem}_{\prec}(p, H \setminus \{p\})$.

(2.2.2) set $H := (H \setminus \{p\}) \cup \{p'\}$

UNTIL $\overline{H} = H$

Step 3 RETURN H

Lemma 4.9. Let \prec_{σ} and \prec_{ω} be monomial orders for the ideal \mathfrak{I} with properties as in Assumptions 4.3, and let $\mathcal{G} := \underline{GB}(\mathfrak{I}, \prec_{\sigma})$ be the reduced GB of \mathfrak{I} w.r.t. \prec_{σ} . Let \mathcal{H} be the GB of \mathfrak{I} w.r.t. \prec_{ω} calculated by Algorithm 2 with inputs \mathcal{G} and \prec_{ω} . And let \mathcal{F} be the output of the Interreduce-Algorithm 3 with inputs \mathcal{H} and \prec_{ω} . Then one finds

$$\mathbb{L}_{\prec_{\omega}}^{[X]}(\mathcal{F}) = \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G}) \quad (4)$$

Proof. We prove (by induction) that the claim on \mathcal{F} in (4) holds for all intermediate sets H assigned in Step 1 and Step (2.2.2) of Algorithm 3.

Initially, one has $H = \mathcal{H}$ by assignment, and by Lemma 4.8 one has $\mathbb{L}_{\prec_{\omega}}^{[X]}(\mathcal{H}) = \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$ for the output \mathcal{H} of the Buchberger-algorithm.

For the induction step assume that the claim in (4) holds for some intermediate set H . Let $p \in H$ be the polynomial chosen in Step (2.2). In regard of Step (2.2.1) we examine the following two cases:

Case 1: Let $p \in H \cap \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$.

In this case, we show that there is no other polynomial in H which can reduce p . Assume that there is $g \in H \setminus \{p\}$ where $\text{lt}_{\prec_{\omega}}(g)$ divides $\text{lt}_{\prec_{\omega}}(p)$. First of all, due to $\text{lt}_{\prec_{\omega}}(p) \in \mathbb{K}[X]$ one has $\text{lt}_{\prec_{\omega}}(g) \in \mathbb{K}[X]$ and thus by assumption of induction $p, g \in \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$. Since \mathcal{G} is a reduced GB w.r.t. σ , $\text{lt}_{\prec_{\sigma}}(g)$ does not divide $\text{lt}_{\prec_{\sigma}}(p)$. Due to Corollary 4.5 one has $\text{lt}_{\prec_{\sigma}}(g) = \text{lt}_{\prec_{\omega}}(g)$ and $\text{lt}_{\prec_{\sigma}}(p) = \text{lt}_{\prec_{\omega}}(p)$ this together with the previous statement is a contradiction to the assumption on g . This finally proves that for $p \in \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$ one has $p' = p$ in Step (2.2.1) and thus H does not change in Step (2.2.2).

Case 2: Let $p \in H \setminus \mathbb{L}_{\prec_{\sigma}}^{[X]}(\mathcal{G})$.

In this case, one can prove for $p' := \text{rem}_{\prec_{\omega}}(p, H \setminus \{p\})$ that one has $\text{lt}_{\prec_{\omega}}(p') \notin \mathbb{K}[X] \setminus \{0\}$ analogously to the proof of Lemma 4.8. This in turn proves that one has $\mathbb{L}_{\prec_{\omega}}^{[X]}(H) = \mathbb{L}_{\prec_{\omega}}^{[X]}(H \setminus \{p\} \cup \{p'\})$, which shows that the claim in (4) holds for the new intermediate set $H \setminus \{p\} \cup \{p'\}$. □

4.3.3. Proof of Theorem 1 via perturbation and generic walks

In Theorem 1 we state that for a fixed ideal the set of weight-vectors suitable for elimination forms a star-shaped set with some center F . We prove this by examining what happens along a Gröbner walk from some σ in the set to some τ in F . For generic walks, we will merely use the Lemmas 4.8 and 4.9 to prove Theorem 1. In what follows we will thus have to examine what happens during Gröbner walks $\overline{\sigma\tau}$ which are not generic.

If $\overline{\sigma\tau}$ is not generic, we can resort to the generic case by perturbing σ . The idea of perturbing σ in order to make the walk generic has been already discussed in depth in [1]. The main difference to our work is that here we need to perturb σ (see Figure 3), not only such that the new Gröbner-path $\overline{\sigma'\tau}$ is generic but also at the same time $\overline{\sigma\tau}$ must in the *neighbourhood* of $\overline{\sigma'\tau}$ and σ' needs to be an \mathfrak{J} -EV.

Definition 4.10. (Neighbourhood)

Let $\mathfrak{J} \subseteq \mathbb{K}[X][U]$ be some ideal and let $\nu \in \mathbb{R}_{\geq 0}^{n+m}$ be some weight-vector. Then the *Neighbourhood* of x is defined as the union of Gröbner fans containing ν :

$$\mathcal{N}(\nu) := \bigcup_{\nu \in C_{\prec}(\mathfrak{J})} C_{\prec}(\mathfrak{J}),$$

The neighbourhood of a set of weight-vectors $A \subseteq \mathbb{R}_{\geq 0}^{n+m}$ is defined as

$$\mathcal{N}(A) := \bigcup_{\nu \in A} \mathcal{N}(\nu).$$

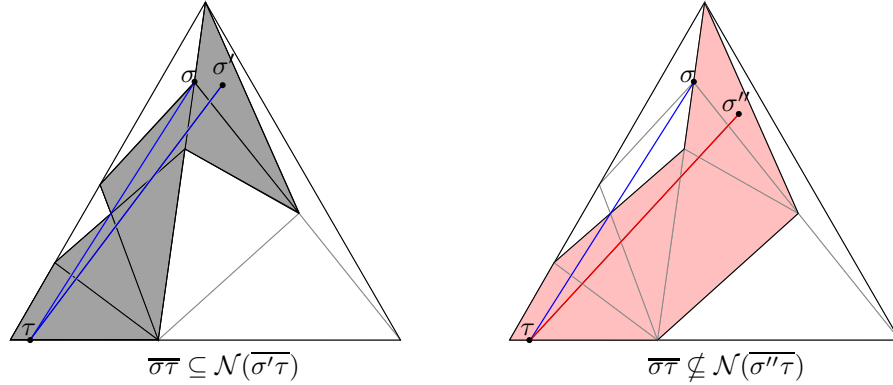


Figure 3: Perturbations to the Gröbner walk $\overline{\sigma\tau}$ with their valid/invalid neighborhoods

Proof of Theorem 1 We have to show the following; let σ, τ be \mathfrak{J} -EVs and let $\tau \in \Omega_u$. Then $\omega \in \overline{\sigma\tau}$ is \mathfrak{J} -EV, too.

In the following let \prec_τ be a monomial-order refining τ , i.e. $\tau \in C_{\prec_\tau}(\mathfrak{J})$.

Case 1: Assume that $\overline{\sigma\tau}$ is a generic Gröbner-path. By definition this means that σ is contained in the interior of some Gröbner cone $C_{\prec_\sigma}(\mathfrak{J})$, where \prec_σ is

an \mathfrak{J} -EO. Moreover, by being generic, $\overline{\sigma\tau}$ only passes through the interior of Gröbner cones or through interior-points of their facets.

Define $\prec_\omega := (\omega \mid \prec_\tau)$, note that this implies $\omega \in C_{\prec_\omega}(\mathfrak{J})$. The reduced Gröbner basis $GB(\mathfrak{J}, \prec_\omega)$ can be calculated via the Algorithms 2 and 3. Using Lemma 4.8 and Lemma 4.9, one finds

$$\mathbb{L}_{\prec_\sigma}^{[X]}(GB(\mathfrak{J}, \prec_\sigma)) = \mathbb{L}_{\prec_\omega}^{[X]}(GB(\mathfrak{J}, \prec_\omega)) \subseteq \mathbb{K}[X].$$

This proves by Definition 2.9 that \prec_ω is an \mathfrak{J} -EO, since for all $g \in GB(\mathfrak{J}, \prec_\omega)$ one has $g \in \mathbb{K}[X]$. Therefore by Definition 2.9 ω is an \mathfrak{J} -EV, since $\omega \in C_{\prec_\omega}$.

Case 2: Assume that $\overline{\sigma\tau}$ is not a generic Gröbner-path.

By Definition 2.9, there is some \mathfrak{J} -EO \prec_σ with $\sigma \in C_{\prec_\sigma}(\mathfrak{J})$. It is straight forward to see that one can perturb σ to σ' such that one has the following three properties: Namely that σ' is in the interior of $C_{\prec_\sigma}(\mathfrak{J})$, $\overline{\sigma'\tau}$ is generic and $\overline{\sigma\tau} \subseteq \mathcal{N}(\overline{\sigma'\tau})$ holds.

Since now $\overline{\sigma'\tau}$ is generic, we conclude from the analysis of Case 1 that for any $\omega \in \overline{\sigma'\tau}$ the order $(\omega \mid \prec_\tau)$ is an \mathfrak{J} -EO.

Correspondingly, the vectors in all Gröbner cones $C_{(\omega \mid \prec_\tau)}(\mathfrak{J})$ which comprise the neighbourhood of $\overline{\sigma'\tau}$ are \mathfrak{J} -EVs.

Due to $\overline{\sigma\tau} \subseteq \mathcal{N}(\overline{\sigma'\tau})$ this implies that any $\omega \in \overline{\sigma\tau}$ is an \mathfrak{J} -EV. \square

5. Conclusion and Outlook

The work of Tran in both [13] and [12] provide proper algorithms to make use of Gröbner walks in the elimination of variables from polynomial ideals. Tran’s approach even simplifies perturbing the corresponding walk in order to obtain a generic walk.

Our results refine this work. We provide a geometric interpretation of the set of ideal-specific elimination vectors. More precisely we prove that these weight-vectors form a star-shaped region. More surprisingly, we show that the corresponding region in general is not convex.

Finally, we redefine Tran’s stopping criterion and show that this yields a true improvement over Tran’s original stopping criterion. Tran’s criterion stops the walk when reaching a Gröbner cone containing the target weight-vector τ , which in turn is part of the boundary of the Gröbner fan. In contrast to this, we show that for some polynomial ideals one can terminate the Gröbner walk in some “interior” Gröbner cone, namely a cone whose intersection with the boundary of the Gröbner fan is just the origin. To this end we provide an example ideal \mathfrak{J} , for which there is an \mathfrak{J} -specific elimination order \prec , whose Gröbner cone $C_{\prec}(\mathfrak{J})$ intersects the boundary of the Gröbner fan in the origin only.

A possible improvement to our work would be to check whether the star shapedness of the region of interest gives rise to cleverly changing the direction of the walk, leading to a more efficient zig-zag-walk. More precisely one would like to answer the following:

If, in some step of the Gröbner walk, the current Gröbner cone borders (via a facet) to some cone of an ideal-specific elimination order, one could of course terminate the walk with a single step. Is it possible to cheaply determine such situations from the current Gröbner basis?

References

- [1] Amrhein, B., Gloor, O., Küchlin, W., 1997. On the walk. Theoretical Computer Science 187, 179–202.
- [2] Buchberger, B., 1965. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Ph.D. thesis. Leopold-Franzens-Universität Innsbruck.
- [3] Buchberger, B., 1988. Applications of gröbner bases in non-linear computational geometry, in: Proceedings of the International Symposium on Trends in Computer Algebra, Springer-Verlag, London, UK. pp. 52–80.
- [4] Collart, S., Kalkbrener, M., Mall, D., 1997. Converting bases with the gröbner walk. Journal of Symbolic Computation 24, 465–469.

- [5] Cox, D., Little, J., O'Shea, D., 1992. Ideals, Varieties, and Algorithms. Undergraduate Texts in Mathematics, Springer-Verlag, New York.
- [6] Fukuda, K., Jensen, A.N., Lauritzen, N., Thomas, R., 2007. The generic gröbner walk. *Journal of Symbolic Computation* 42, 298–312.
- [7] Kalkbrenner, M., 1991. Implicitization of rational parametric curves and surfaces, in: AAECC-8, Proceedings of the 8th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Springer-Verlag, London, UK. pp. 249–259.
- [8] Mora, T., Robbiano, L., 1988. The gröbner fan of an ideal. *Journal of Symbolic Computation* 6, 183–208.
- [9] Salmon, G., 1964. *Lessons Introductory to the Modern Higher Algebra*, fifth ed. Chelsea Publishing Company, Bronx, New York.
- [10] Sederberg, T., Anderson, D., Goldman, R.N., 1984. Implicit representation of parametric curves and surfaces. *Computer Vision, Graphics and Image Processing* 28, 72–84.
- [11] Sylvester, J., 1904. *The collected mathematical papers of James Joseph Sylvester*. Cambridge University Press, Cambridge, England.
- [12] Tran, Q.N., 2004. Efficient gröbner walk conversion for implicitization of geometric objects. *Journal of Computer Aided Geometric Design* 21, 837–857.
- [13] Tran, Q.N., 2007. A new class of term orders for elimination. *Journal of Symbolic Computation* 42, 533–548.